CLAIMS

What is claimed is:

1. A method for tracing a denial-of-service attack on a victim machine back towards its source, comprising steps of:

operating a traceback program on at least one path to receive two input parameters, (a) an IP address (v) of the victim machine and (b) an IP address (r) of a router that is immediately upstream of the victim machine;

determining a set of routers that are neighbors (n) of r;

for each neighbor n of r, determining if r is n's next-hop for traffic addressed to v, or to a network that v is on, where node n's next-hop for traffic addressed to v is the IP address of the node that n will forward a packet to if the destination address in the packet is v;

if r is not n's next-hop for traffic addressed to v, skip over n and query the next neighbor of r, while if r is n's next-hop for traffic addressed to v, determining an amount of traffic that n is forwarding to r that is addressed to v; and

after determining the identity of the neighbor n of r that is the principal source of packets flowing to r that are addressed to v, continuing one node further upstream from the determined neighbor n of r that is the principal source of packets flowing to r that are addressed to v, and continuing to traceback through interconnected routers until a source of denial-of-service attack packets to v is determined or until further traceback is not possible.

2. A method as in claim 1, wherein the step of determining the set of neighbors comprises a step of sending at least one query to r to obtain information from a MIB that stores IP addresses of routers that are neighbors of r.

3. A method as in claim 1, wherein the step of determining if r is n's next-hop for traffic addressed to v comprises a step of sending at least one query to router n.

4. A method as in claim 3, wherein the step of sending at least one query queries

an IP Forwarding Table MIB of router n.

5. A method as in claim 1, wherein the step of determining an amount of traffic comprises a step of sending at least one message to a neighbor router n for determining a count of packets that router n is sending to router r that are addressed to v or to a network on which v resides.

6. A method as in claim 1, and further comprising a step of establishing a black hole host route to v as close as is possible to the source of the denial-of-service attack packets.

7. A method as in claim 1, and further comprising a step of establishing a special host route to v using the same next hop as an existing route, the special host route tracking changes in the existing route such that when a next hop for the existing route changes, the next hop for the host route changes similarly.

8. A method as in claim 1, and further comprising a step of establishing a rate-limit for packets addressed to v as close as is possible to the source of the denial-of-service attack packets.

9. A backtracking unit for tracing a denial-of-service attack on a victim machine back towards its source or sources, comprising a data processor responsive to a traceback computer program stored on a computer-readable media for receiving a first input parameter of an IP address (v) of the victim machine and a second input parameter of an IP address (r) of a router that is immediately upstream of the victim machine, said traceback computer program controlling operation of said data processor to determine a set of routers that are neighbors (n) of r and, for each neighbor n of r, to determine if r is n's next-hop for traffic addressed to v, where node n's next-hop for traffic addressed to v is the IP address of the node that n will forward a packet to if the destination address in the packet is v, said traceback computer program further controlling operation of said data processor for the case where r is not n's next-hop for traffic addressed to v, to skip over n and to query the next neighbor of r, while for the case where r is n's next-hop for traffic addressed to v, to determine an amount of traffic that n is forwarding to r that is addressed to v, and after determining the identity of the neighbor n of r that is the principal source of packets flowing to r that are addressed to v or to a network to which v is connected, for continuing further upstream from the determined neighbor n of r that is the principal source of packets flowing to r that are addressed to v to continue to

traceback through interconnected routers until a source of denial-of-service attack packets to v is determined, or until further traceback is not possible.

10. A backtracking unit as in claim 9, wherein said data processor operates to send at least one query to r to obtain information from a MIB that stores IP addresses of routers that are neighbors of r.

11. A backtracking unit as in claim 9, wherein said data processor operates to send at least one query to an IP Forwarding Table MIB of router n.

12. A backtracking unit as in claim 9, wherein said data processor, while determining an amount of traffic that n is forwarding to r that is addressed to v, operates under control of said traceback computer program to send at least one message to at least one neighbor router n to determine a count of packets that router n is sending to router r that are addressed to v or to the network to which v is connected.

13. A backtracking unit as in claim 9, wherein said data processor further operates to establish a black hole host route to v as close as is possible to the source of the denial-of-service attack packets.

14. A backtracking unit as in claim 9, wherein said data processor further operates to establish a special host route to v using the same next hop as an existing route, the special host route tracking changes in the existing route such that when a next hop for the existing route changes, the next hop for the host route changes similarly.

15. A backtracking unit as in claim 9, wherein said data processor further operates to establish a rate-limit for packets addressed to v as close as is possible to the source of the denial-of-service attack packets.

16 A method for determining an identity of a source of undesirable packets received from a data communications network, comprising steps of:

operating a traceback function to receive at least one input parameter, namely a network address (v) of a device receiving the undesirable packets;

determining a set of network routers that are neighbors (n) of a network router

(r) that is coupled to the device immediately upstream of the device; and

querying individual ones of packet routers in order to determine a packet router that is a largest source of packets addressed to v via r, or to a network to which v is connected, and continuing to query packet routers up through a hierarchy of interconnected packet routers until an identity of a source of the undesirable packets is discovered or until further backtracking is not possible.

17. A method as in claim 16, wherein the steps of determining and querying each comprise a step of sending queries to the data communications network.

18. A method as in claim 16, wherein the step of querying comprises steps of:

sending a first network message to a packet router for instructing the packet router to determine a number of packets that it is sending addressed to v; and

sending a second network message to the packet router to query the packet router for the determined number.

19. A method as in claim 16, wherein the step of querying comprises a step of sending at least one message to a packet router for determining a number of packets being forwarded to or towards v.

20. A method as in claim 16, and further comprising a step of establishing at least one of a black hole host route to v as close as is possible to the source of the undesirable packets, establishing a special host route to v using the same next hop as an existing route, the special host route tracking changes in the existing route such that when a next hop for the existing route changes, the next hop for the host route changes similarly, and establishing a rate-limit for packets addressed to v as close as is possible to the source of the denial-of-service attack packets.

21. A method as in claim 16, wherein the step of operating the traceback function operates the traceback function on a plurality of selected paths, wherein a particular path is selected based at least on an amount of traffic flowing through the path.